

TRACES OF HIGH POWERS OF THE FROBENIUS CLASS IN THE MODULI SPACE OF HYPERELLIPTIC CURVES

IAKOVOS JAKE CHINIS

ABSTRACT. The Zeta function of a curve C over a finite field may be expressed in terms of the characteristic polynomial of a unitary matrix Θ_C . Following the work of Rudnick [1], we compute the expected value of $\text{tr}(\Theta_C^n)$ over the moduli space of hyperelliptic curves of genus g , over a fixed finite field \mathbb{F}_q , in the limit of large genus. As an application, we compute the expected value of the number of points on C in \mathbb{F}_{q^n} as the genus tends to infinity. We also look at biases in both expected values for small values of n .

1. INTRODUCTION

Let C be a smooth projective curve of genus $g \geq 1$ defined over a fixed finite field \mathbb{F}_q of odd cardinality q . If we let $\#C(\mathbb{F}_{q^n})$ denote the number of points on C in finite extensions \mathbb{F}_{q^n} of degree n of \mathbb{F}_q , then the Zeta function associated to the curve C is defined by

$$(1.1) \quad Z_C(u) := \exp \left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} u^n \right), |u| < \frac{1}{q}.$$

It is known that $Z_C(u)$ is a rational function in u of the form

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)},$$

where $P_C(u) \in \mathbb{Z}[u]$ is a polynomial of degree $2g$, with $P_C(0) = 1$, satisfying the functional equation

$$(1.2) \quad P_C(u) = (qu^2)^g P_C\left(\frac{1}{qu}\right).$$

It was proven by Weil [7] that the zeros of $P_C(u)$ all lie on the circle $|u| = 1/q^{\frac{1}{2}}$. Hence,

$$P_C(u) = \prod_{j=1}^{2g} (1 - q^{\frac{1}{2}} e^{i\theta_j(C)} u),$$

Date: October 22, 2015.

for some angles $\theta_j(C)$, $1 \leq j \leq 2g$, and

$$(1.3) \quad Z_C(u) = \exp \left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} u^n \right) = \frac{\prod_{j=1}^{2g} (1 - q^{\frac{1}{2}} e^{i\theta_j(C)} u)}{(1-u)(1-qu)}.$$

Now, we may define a unitary symplectic matrix $\Theta_C \in \mathrm{USp}(2g)$ by

$$\Theta_{C_{jk}} := \begin{cases} e^{i\theta_j(C)} & \text{if } k = j \\ 0 & \text{otherwise,} \end{cases}$$

for $1 \leq j, k \leq 2g$. Then it is clear that the Zeta function associated to C can be expressed in terms of the characteristic polynomial of Θ_C

$$Z_C(u) = \frac{\det(\mathbb{I} - u\sqrt{q}\Theta_C)}{(1-u)(1-qu)},$$

with Θ_C unique up to conjugacy. We call the conjugacy class of Θ_C the *unitarized Frobenius class* of C .

Let \mathcal{H}_g be the moduli space of hyperelliptic curves of genus g over \mathbb{F}_q ; i.e., the set of hyperelliptic curves given by the affine equation

$$C_Q : y^2 = Q(x),$$

where $Q \in \mathbb{F}_q[x]$ is any squarefree polynomial of degree $2g+1$ or $2g+2$. In this model, the point at infinity is not smooth, but we may consider the smooth portion of C_Q and account for the point at infinity separately; in the smooth model, the point at infinity will be replaced by 0, 1, or 2 points and we get that the number of points at infinity is

$$(1.4) \quad \begin{cases} 0 & \text{if } \deg(Q) \text{ is even and } \mathrm{sgn}(Q) \neq \square \\ 1 & \text{if } \deg(Q) \text{ is odd} \\ 2 & \text{if } \deg(Q) \text{ is even and } \mathrm{sgn}(Q) = \square. \end{cases}$$

Note the relation between equations (1.4) and (2.3); namely, the number of points at infinity is $\lambda_Q + 1$, with λ_Q as in (2.3).

Remark. The smooth model is the closure of C_Q , denoted $\overline{C_Q}$, under the map

$$[1, x, x^2, \dots, x^{g-1}, y] : C_Q \rightarrow \mathbb{P}^{g+2}.$$

One can show that this closure consists of two affine components: the first is C_Q itself and the second is the curve given by $y^2 = x^{2g+2}Q(\frac{1}{x})$. In fact, C_Q is isomorphic to $\overline{C_Q} \cap \{x_0 \neq 0\}$; we refer the reader to Silverman [8].

For any function F on \mathcal{H}_g , we define the expected value of F over \mathcal{H}_g

$$(1.5) \quad \langle F \rangle_{\mathcal{H}_g} := \frac{1}{\#\mathcal{H}_g} \cdot \sum_{C_Q \in \mathcal{H}_g} F(C_Q).$$

In this paper, we study the traces of high powers of the Frobenius class of C_Q over \mathcal{H}_g over a fixed finite field \mathbb{F}_q of odd cardinality q as $g \rightarrow \infty$. In particular, we concern ourselves with the expected values of $\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g}$ as $g \rightarrow \infty$ and we compare our work with the Random Matrix results of [3].

From the work of Diaconis and Shahshahani [3], the expected value of the traces of powers over the unitarized symplectic group $\text{USp}(2g)$ is given by

$$(1.6) \quad \int_{\text{USp}(2g)} \text{tr}(U^n) du = \begin{cases} -\eta_n & \text{if } 1 \leq n \leq 2g \\ 0 & \text{if } n > 2g, \end{cases}$$

where

$$\eta_n = \begin{cases} 1 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd.} \end{cases}$$

We will prove the following theorem and the accompanying corollary:

Theorem 1.1. *For n odd,*

$$\langle \text{tr}(\Theta_C^n) \rangle_{\mathcal{H}_g} = 0,$$

and for n even,

$$\langle \text{tr}(\Theta_C^n) \rangle_{\mathcal{H}_g} = \frac{1}{q^{\frac{n}{2}}} \cdot \sum_{\substack{\deg(P) \mid \frac{n}{2} \\ \deg(P) \neq 1}} \frac{\deg(P)}{|P| + 1} + O(gq^{\frac{-g}{2}}) + \begin{cases} -1 & 0 < n < 2g \\ -1 - \frac{1}{q^2 - 1} & n = 2g \\ O(nq^{\frac{n}{2} - 2g}) & 2g < n, \end{cases}$$

where the sum is over all monic irreducible polynomials $P \in \mathbb{F}_q[x]$ and where $|P| := q^{\deg(P)}$.

Corollary 1.2. *If n is odd, then*

$$\langle \text{tr}(\Theta_C^n) \rangle_{\mathcal{H}_g} = \int_{\text{USp}(2g)} \text{tr}(U^n) dU.$$

For n even with $3 \log_q(g) < n < 4g - 5 \log_q(g)$ and $n \neq 2g$,

$$\langle \text{tr}(\Theta_C^n) \rangle_{\mathcal{H}_g} = \int_{\text{USp}(2g)} \text{tr}(U^n) dU + o\left(\frac{1}{g}\right).$$

In [1], Rudnick considers the mean value of $\text{tr}(\Theta_C^n)$ over a family of hyperelliptic curves given by the affine equation $C : y^2 = Q(x)$ where $Q(x) \in \mathcal{F}_{2g+1}$, with

$$\mathcal{F}_{2g+1} := \{f \in \mathbb{F}_q[x] : f \text{ monic, squarefree, and } \deg(f) = 2g + 1\},$$

and obtains that

$$\langle \text{tr}(\Theta_C^n) \rangle_{\mathcal{F}_{2g+1}} = \eta_n \frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P) \mid \frac{n}{2}} \frac{\deg(P)}{|P|+1} + O(gq^{-g}) + \begin{cases} -\eta_n & 0 < n < 2g \\ -1 - \frac{1}{q-1} & n = 2g \\ O(nq^{\frac{n}{2}-2g}) & 2g < n; \end{cases}$$

in particular, if $3 \log_q(g) < n < 4g - 5 \log_q(g)$ and $n \neq 2g$, then

$$\langle \text{tr}(\Theta_C^n) \rangle_{\mathcal{F}_{2g+1}} = \int_{\text{USp}(2g)} \text{tr}(U^n) dU + o\left(\frac{1}{g}\right).$$

Rudnick then points out that there is a slight deviation in $\langle \text{tr}(\Theta_C^n) \rangle_{\mathcal{F}_{2g+1}}$ from the Random Matrix Theory results for small values of n and for $n = 2g$; namely,

$$\langle \text{tr}(\Theta_C^2) \rangle_{\mathcal{F}_{2g+1}} \sim \int_{\text{USp}(2g)} \text{tr}(U^2) dU + \frac{1}{q+1}$$

and

$$\langle \text{tr}(\Theta_C^{2g}) \rangle_{\mathcal{F}_{2g+1}} \sim \int_{\text{USp}(2g)} \text{tr}(U^{2g}) dU - \frac{1}{q-1}.$$

By considering the average value of $\text{tr}(\Theta_C^n)$ over \mathcal{H}_g , we no longer get a deviation from the RMT results for $n = 2$ and the deviation at $n = 2g$ diminishes:

$$\langle \text{tr}(\Theta_C^2) \rangle_{\mathcal{H}_g} \sim \int_{\text{USp}(2g)} \text{tr}(U^2) dU$$

and

$$\langle \text{tr}(\Theta_C^{2g}) \rangle_{\mathcal{H}_g} \sim \int_{\text{USp}(2g)} \text{tr}(U^{2g}) dU - \frac{1}{q^2 - 1}.$$

Furthermore, our results for odd n are exact and coincide with the RMT results for all values of g . At first glance, this may seem counterintuitive as one expects to have an error term, as in the even case and as in [1]. Using another approach, one can quickly verify the first result of Theorem 1.1 (this is done in section 10).

Now, we may apply Theorem 1.1 to compute the average number of points on C_Q in finite extensions \mathbb{F}_{q^n} of \mathbb{F}_q over \mathcal{H}_g , denoted $\langle \#C(\mathbb{F}_{q^n}) \rangle_{\mathcal{H}_g}$:

By taking logarithmic derivatives in (1.3),

$$\begin{aligned} \#C_Q(\mathbb{F}_{q^n}) &= q^n + 1 - q^{\frac{n}{2}} \sum_{j=1}^{2g} e^{in\theta_j(C_Q)} \\ &= q^n + 1 - q^{\frac{n}{2}} \text{tr}(\Theta_{C_Q}^n). \end{aligned}$$

In fact,

$$\begin{aligned} \langle \#C_Q(\mathbb{F}_{q^n}) \rangle_{\mathcal{H}_g} &= q^n + 1 - q^{\frac{n}{2}} \langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} \\ &\sim q^n + \eta_n q^{\frac{n}{2}} + 1 - \eta_n \sum_{\substack{\deg(P) \mid \frac{n}{2} \\ \deg(P) \neq 1}} \frac{\deg(P)}{|P| + 1}. \end{aligned}$$

More precisely,

Corollary 1.3. (i) *If n is odd, then*

$$\langle \#C_Q(\mathbb{F}_{q^n}) \rangle_{\mathcal{H}_g} = q^n + 1.$$

(ii) *If n is even, then*

$$\langle \#C_Q(\mathbb{F}_{q^n}) \rangle_{\mathcal{H}_g} \sim q^n + q^{\frac{n}{2}} + 1 - \sum_{\substack{\deg(P) \mid \frac{n}{2} \\ \deg(P) \neq 1}} \frac{\deg(P)}{|P| + 1}.$$

Once again, our results for odd n are exact and hold for all values of g . Although we continue to get deviations from the RMT results for even $n \geq 4$, our results hold for $n = 2$ and our deviations are different from those obtained in [1].

Another approach to computing $\langle \#C_Q(\mathbb{F}_{q^n}) \rangle_{\mathcal{H}_g}$ is the work of Alzahrani [5] who uses the distribution of points on \mathcal{H}_g over \mathbb{F}_q in \mathbb{F}_{q^n} . Using these methods, the results of Alzahrani agree with the Corollary above (albeit with a larger error term).

Finally, we would like to mention that some of the computations done in sections 3 through 8 were done independently by E. Lorenzo, G. Meleleo, and P. Milione in their study of statistics for biquadratic curves; their work is collected in [9].

2. BACKGROUND

In this section, we establish some notation and we introduce the main results of [1]. Since the majority of what follows is based off of the work in [1], we use the same notation and list important results for the convenience of the reader. We use [2] as a general reference.

Throughout this paper, \mathbb{F}_q is a fixed finite field of odd cardinality q , P represents monic irreducible polynomials in $\mathbb{F}_q[x]$, and Q will be used to denote squarefree polynomials of degree $2g + 1$ or $2g + 2$ with $g \geq 1$. Unless otherwise stated, it is understood that sums and products are over all monic elements in $\mathbb{F}_q[x]$; in the case where a sum involves elements $B \in \mathbb{F}_q[x]$ that are not necessarily monic, we write the sum over B n.n.m..

Given any polynomial $D \in \mathbb{F}_q[x]$ that is not a perfect square, we define the quadratic character χ_D by the quadratic residue symbol for $\mathbb{F}_q[x]$

$$\chi_D(f) := \left(\frac{D}{f} \right),$$

where f is any monic polynomial in $\mathbb{F}_q[x]$.

The Zeta function associated to the hyperelliptic curve $C_Q : y^2 = Q(x)$ is then given by

$$Z_{C_Q}(u) = L^*(u, \chi_Q) \zeta_q(u),$$

where

$$\zeta_q(u) := \frac{1}{(1-u)(1-qu)}$$

is the Zeta function of $\mathbb{F}_q(x)$ and where

$$(2.1) \quad L^*(u, \chi_Q) := (1 - \lambda_Q \cdot u)^{-1} \prod_{P \in \mathbb{F}_q[x]} (1 - \chi_Q(P) \cdot u^{\deg(P)})^{-1}$$

$$(2.2) \quad = \det(\mathbb{I} - u\sqrt{q} \cdot \Theta_{C_Q}),$$

with

$$(2.3) \quad \lambda_Q := \begin{cases} -1 & \text{if } \deg(Q) \text{ is even and } \text{sgn}(Q) \neq \square \\ 0 & \text{if } \deg(Q) \text{ is odd} \\ 1 & \text{if } \deg(Q) \text{ is even and } \text{sgn}(Q) = \square, \end{cases}$$

which relates to the count in equation (1.4).

Taking logarithmic derivatives in equations (2.1) and (2.2), we see that

$$(2.4) \quad \sum_{j=1}^{2g} e^{in\theta_j(C_Q)} = \text{tr}(\Theta_{C_Q}^n) = -\frac{\lambda_Q^n}{q^{\frac{n}{2}}} - \frac{1}{q^{\frac{n}{2}}} \sum_{\deg(f)=n} \Lambda(f) \chi_Q(f),$$

where

$$\Lambda(f) := \begin{cases} \deg(P) & \text{if } f = P^k \\ 0 & \text{otherwise} \end{cases}$$

is the *von Mangoldt* function.

Let

$$\mathcal{F}_d := \{f \in \mathbb{F}_q[x] : f \text{ monic, squarefree, and } \deg(f) = d\}$$

and let

$$\widehat{\mathcal{F}}_d := \{f \in \mathbb{F}_q[x] : f \text{ squarefree and } \deg(f) = d\}.$$

Then

$$\#\widehat{\mathcal{F}}_d = (q-1)\#\mathcal{F}_d$$

and it is easy to see that (see Lemma 3 of [6], for example)

$$\#\mathcal{F}_d = \begin{cases} (1 - \frac{1}{q})q^d, & d \geq 2 \\ q, & d = 1. \end{cases}$$

Using these sets of polynomials, every curve in the moduli space of hyperelliptic curves of genus g has a model $C_Q : y^2 = Q(x)$, where $Q \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$.

Now, let \mathcal{F} be any family of squarefree polynomials of degree d in $\mathbb{F}_q[x]$. For any function F on \mathcal{F} , we define the expected value of F over \mathcal{F}

$$\langle F \rangle_{\mathcal{F}} := \frac{1}{\#\mathcal{F}} \cdot \sum_{Q \in \mathcal{F}} F(Q).$$

In particular,

$$(2.5) \quad \langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}} = \frac{1}{\#\mathcal{F}} \cdot \sum_{Q \in \mathcal{F}} \left(-\frac{\lambda_Q^n}{q^{\frac{n}{2}}} - \frac{1}{q^{\frac{n}{2}}} \sum_{\deg(f)=n} \Lambda(f) \chi_Q(f) \right).$$

In [1], Rudnick averages the trace over $\mathcal{F} = \mathcal{F}_{2g+1}$. We begin by considering the average over $\mathcal{F} = \mathcal{F}_{2g+2}$ and then obtain the average over \mathcal{H}_g by combining our results and also considering the contribution of the point at infinity which differs on each component $\widehat{\mathcal{F}}_{2g+1}, \widehat{\mathcal{F}}_{2g+2}$.

Let μ denote the Möbius function. Since

$$\sum_{A^2|Q} \mu(A) = \begin{cases} 1 & \text{if } Q \text{ is squarefree} \\ 0 & \text{otherwise,} \end{cases}$$

we may compute the expected value of F by summing over all elements of degree d in $\mathbb{F}_q[x]$ and sieving out the squarefree terms; namely,

$$(2.6) \quad \langle F(Q) \rangle_{\mathcal{F}} = \frac{1}{\#\mathcal{F}} \sum_{2\alpha+\beta=d} \sum_{\substack{\deg(B)=\beta \\ B \text{ n.n.m.}}} \sum_{\deg(A)=\alpha} \mu(A) F(A^2 B).$$

For all $A, B \in \mathbb{F}_q[x]$,

$$\chi_{A^2 B}(f) = \left(\frac{B}{f}\right) \cdot \left(\frac{A}{f}\right)^2 = \begin{cases} \left(\frac{B}{f}\right) & \text{if } (A, f) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

With that said, taking $F(Q) = \chi_Q$ in equation (2.6),

$$\langle \chi_Q(f) \rangle_{\mathcal{F}} = \frac{1}{\#\mathcal{F}} \cdot \sum_{\substack{2\alpha+\beta=d \\ \alpha, \beta \geq 0}} \sigma(f; \alpha) \sum_{\substack{\deg(B)=\beta \\ B \text{ n.n.m.}}} \left(\frac{B}{f}\right),$$

where

$$\sigma(f; \alpha) := \sum_{\substack{\deg(A)=\alpha \\ (A,f)=1}} \mu(A).$$

We are now in a position to provide the necessary results from [1]:

For any $P \in \mathbb{F}_q[x]$ with $\deg(P) = n$, we define

$$\sigma_n(\alpha) := \sigma(P^k; \alpha) = \sum_{\substack{\deg(A)=\alpha \\ (A,P^k)=1}} \mu(A) = \sum_{\substack{\deg(A)=\alpha \\ (A,P)=1}} \mu(A) = \sigma(P; \alpha).$$

Lemma 2.1. [1, Lemma 4] (i) For $n = 1$,

$$(2.7) \quad \sigma_1(0) = 1, \sigma_1(\alpha) = 1 - q \quad \forall \alpha \geq 1.$$

(ii) If $n \geq 2$, then

$$(2.8) \quad \sigma_n(\alpha) = \begin{cases} 1 & \alpha \equiv 0 \pmod{n} \\ -q & \alpha \equiv 1 \pmod{n} \\ 0 & \text{otherwise.} \end{cases}$$

Recall that the Dirichlet L-series associated to χ_Q , denoted $L(u, \chi_Q)$ for $|u| < 1/q$, is a polynomial in u of degree at most $\deg(Q) - 1$ (see Proposition 4.3 of [2], for example). In fact,

$$L(u, \chi_Q) := \prod_{P \in \mathbb{F}_q[x]} (1 - \chi_Q(P) \cdot u^{\deg(P)})^{-1} = \sum_{\beta \geq 0} A_Q(\beta) u^\beta,$$

where

$$A_Q(\beta) := \sum_{\deg(B)=\beta} \chi_Q(B)$$

and $A_Q(\beta) = 0$ for $\beta \geq \deg(Q)$.

Let

$$S(\beta; n) := \sum_{\deg(P)=n} \sum_{\deg(B)=\beta} \left(\frac{B}{P} \right).$$

By the *Law of Quadratic Reciprocity* [2],

$$S(\beta; n) = (-1)^{\frac{q-1}{2}\beta n} \sum_{\deg(P)=n} A_P(\beta)$$

$$(2.9) \quad \Rightarrow S(\beta; n) = 0 \quad \forall n \leq \beta.$$

We let $\pi_q(n)$ denote the number of monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$. From the *Prime Polynomial Theorem* [2],

$$\begin{aligned}\pi_q(n) &:= \#\{P \in \mathbb{F}_q[x] : \deg(P) = n\} \\ &= \frac{q^n}{n} + O\left(\frac{q^{\frac{n}{2}}}{n}\right).\end{aligned}$$

Lemma 2.2. [1, Proposition 7] (i) n odd, $0 \leq \beta \leq n-1$:

$$(2.10) \quad S(\beta; n) = q^{\beta - \frac{n-1}{2}} S(n-1-\beta; n)$$

and

$$(2.11) \quad S(n-1; n) = \pi_q(n) q^{\frac{n-1}{2}}.$$

(ii) n even, $1 \leq \beta \leq n-2$:

$$(2.12) \quad S(\beta; n) = q^{\beta - \frac{n}{2}} \left(-S(n-1-\beta; n) + (q-1) \sum_{j=0}^{n-\beta-2} S(j; n) \right)$$

and

$$(2.13) \quad S(n-1; n) = -\pi_q(n) q^{\frac{n-2}{2}}.$$

Lemma 2.3. [1, Lemma 8] If $\beta < n$, then

$$(2.14) \quad S(\beta; n) = \eta_\beta \pi_q(n) q^{\frac{\beta}{2}} + O\left(\frac{\beta}{n} q^{\frac{n}{2} + \beta}\right),$$

where $\eta_\beta = 1$ for β even and $\eta_\beta = 0$ for β odd.

3. IMPROVED ESTIMATE FOR $S(\beta; n)$ WHEN β IS EVEN

Initially, we concern ourselves with $\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+2}}$; in doing so, we need to estimate $S(\beta; n)$ for when β is even (see sections 5 and 7). The following theorem makes use of Lemmas 2.2 and 2.3; it is the analogous result to Proposition 9 of [1] (since Rudnick considers the average value over \mathcal{F}_{2g+1} , estimates for $S(\beta; n)$ in [1] involve β odd). Furthermore, this result will allow us to compute $\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+2}}$ for n near $4g$ (just as Proposition 9 in [1] allows Rudnick to compute $\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+1}}$ for n near $4g$).

Theorem 3.1. If β is even, $\beta \neq 0$, and $\beta < n$, then

$$(3.1) \quad S(\beta; n) = \pi_q(n) (q^{\frac{\beta}{2}} - \eta_n q^{\beta - \frac{n}{2}}) + O(q^n),$$

where

$$\eta_n = \begin{cases} 1 & n \text{ even} \\ 0 & n \text{ odd.} \end{cases}$$

Remarks. (i) The result above is essentially the same as Proposition 9 in [1] with one additional term; namely, $\pi_q(n)q^{\frac{\beta}{2}}$.

(ii) As Rudnick points out in [1], the main tool in proving Theorem 3.1 is duality; it allows us to improve the error term in estimates of $S(\beta; n)$ and to get results holding for $n < 4g$ and not only for $n < 2g$. We would like to mention that the duality present in our character sums $S(\beta; n)$ is based on the functional equation (1.2)

$$L^*(u, \chi_P) = (uq^2)^{\lfloor \frac{\deg(P)-1}{2} \rfloor} L^*\left(\frac{1}{qu}, \chi_P\right),$$

for prime characters χ_P (see the proof of Proposition 7 in [1]).

Proof. (i) If n is odd, we apply (2.10) to $S(\beta; n)$ and then apply (2.14) to $S(n-1-\beta; n)$:

$$\begin{aligned} S(\beta; n) &= q^{\beta - \frac{n-1}{2}} S(n-1-\beta; n) \\ &= q^{\beta - \frac{n-1}{2}} \left(\pi_q(n) q^{\frac{n-1-\beta}{2}} + O\left(\frac{n-1-\beta}{n} q^{\frac{n}{2}+n-1-\beta}\right) \right) \\ &= \pi_q(n) q^{\frac{\beta}{2}} + O(q^n). \end{aligned}$$

(ii) If n is even, we apply (2.12) to $S(\beta; n)$ and then apply (2.14) to $S(n-1-\beta; n)$:

$$\begin{aligned} S(\beta; n) &= q^{\beta - \frac{n}{2}} \left(-S(n-1-\beta; n) + (q-1) \sum_{j=0}^{n-\beta-2} S(j; n) \right) \\ &= q^{\beta - \frac{n}{2}} \left(O\left(\frac{n-1-\beta}{n} q^{\frac{n}{2}+n-1-\beta}\right) + (q-1) \sum_{j=0}^{n-\beta-2} \left(\eta_j \pi_q(n) q^{\frac{j}{2}} + O\left(\frac{j}{n} q^{\frac{n}{2}+j}\right) \right) \right). \end{aligned}$$

The two error terms are $O(q^n)$. Since both n and β are even, $n-\beta-2$ is even and we may rewrite the main term as

$$\pi_q(n) q^{\beta - \frac{n}{2}} (q-1) \sum_{j=0}^{\frac{n-\beta-2}{2}} q^j.$$

Hence,

$$\begin{aligned} S(\beta; n) &= \pi_q(n) q^{\beta - \frac{n}{2}} (q-1) \sum_{j=0}^{\frac{n-\beta-2}{2}} q^j + O(q^n) \\ &= \pi_q(n) q^{\beta - \frac{n}{2}} (q^{\frac{n-\beta}{2}} - 1) + O(q^n) \\ &= \pi_q(n) (q^{\frac{\beta}{2}} - q^{\beta - \frac{n}{2}}) + O(q^n). \end{aligned}$$

□

 4. COMPUTING $\text{tr}(\Theta_{C_Q}^n)$ FOR $Q \in \mathcal{F}_{2g+2}$

For the time being, we restrict ourselves to \mathcal{F}_{2g+2} . Let $Q \in \mathcal{F}_{2g+2}$ and consider the curve $C_Q : y^2 = Q(x)$. The trace of the powers of Θ_{C_Q} is given by equation (2.4):

$$(4.1) \quad \text{tr}(\Theta_{C_Q}^n) = -\frac{1}{q^{\frac{n}{2}}} - \frac{1}{q^{\frac{n}{2}}} \sum_{\deg(f)=n} \Lambda(f) \chi_Q(f)$$

$$(4.2) \quad = -\frac{1}{q^{\frac{n}{2}}} - \frac{1}{q^{\frac{n}{2}}} \sum_{\substack{P,k \\ \deg(P^k)=n}} \deg(P) \chi_Q(P^k)$$

$$(4.3) \quad = -\frac{1}{q^{\frac{n}{2}}} + \mathcal{P}_n + \square_n + \mathbb{H}_n,$$

where \mathcal{P}_n corresponds to $k = 1$, \square_n corresponds to the sum over all k even, and \mathbb{H}_n corresponds to the sum over all odd $k \geq 3$.

In the next three sections, we continue to use Rudnick's methods in order to compute \mathcal{P}_n , \square_n , and \mathbb{H}_n . Not surprisingly, our results will only slightly differ from Rudnick's. The addition of $-1/q^{\frac{n}{2}}$ from (1.1) will be the main difference. We will also have different cut-off points for n when estimating \mathcal{P}_n (see section 5.3 of [1]).

 5. CONTRIBUTION OF THE PRIMES: \mathcal{P}_n

The contribution of the primes in (4.1) is given by:

$$\mathcal{P}_n = -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P)=n} n \chi_Q(P).$$

So,

$$\begin{aligned} \langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} &= \frac{-n}{(q-1)q^{2g+1+\frac{n}{2}}} \sum_{\deg(P)=n} \sum_{2\alpha+\beta=2g+2} \sigma_n(\alpha) \sum_{\deg(B)=\beta} \left(\frac{B}{P} \right) \\ &= \frac{-n}{(q-1)q^{2g+1+\frac{n}{2}}} \sum_{2\alpha+\beta=2g+2} \sigma_n(\alpha) S(\beta; n). \end{aligned}$$

From Lemma 2.1, if $n > g+1$, then

$$\begin{aligned} \sigma_n(\alpha) \neq 0 &\Rightarrow (\alpha \equiv 0 \pmod{n} \text{ or } \alpha \equiv 1 \pmod{n}) \\ &\Rightarrow (\alpha = 0 \text{ or } \alpha = 1), \end{aligned}$$

which follows from the fact that $0 \leq \alpha \leq g + 1$.

Since $\sigma_n(0) = 1$ and $\sigma_n(1) = -q$, when $n > g + 1$, we have

$$\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} = \frac{-n}{(q-1)q^{2g+1+\frac{n}{2}}} (S(2g+2; n) - qS(2g; n)).$$

We now compute $\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}}$ by considering the case $n \leq g + 1$ and the case $n > g + 1$, which we break into four (non-distinct) ranges:

(i) $n \leq g + 1$: If $S(\beta; n) \neq 0$, then $\beta < n$; since β is even,

$$\begin{aligned} S(\beta; n) &= \pi_q(n)q^{\frac{\beta}{2}} + O\left(\frac{\beta}{n}q^{\beta+\frac{n}{2}}\right) \\ &= \frac{q^{n+\frac{\beta}{2}}}{n} + O\left(\frac{q^{\frac{n}{2}+\frac{\beta}{2}}}{n}\right) + O\left(\frac{\beta}{n}q^{\beta+\frac{n}{2}}\right). \end{aligned}$$

Then

$$S(\beta; n) \ll \frac{\beta}{n}q^{n+\beta},$$

which implies that

$$\begin{aligned} \langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} &\ll \frac{n}{q^{2g+\frac{n}{2}}} \sum_{\beta < n} \frac{\beta}{n} q^{\beta+n} \\ &\ll \frac{n}{q^{2g+\frac{n}{2}}} q^{2n} = nq^{\frac{3n}{2}-2g} \ll gq^{\frac{-g}{2}}. \end{aligned}$$

(ii) $g + 1 < n < 2g + 1$: Since $2g + 2, 2g \geq n$, $S(2g + 2; n) = S(2g; n) = 0$. Hence,

$$\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} = \frac{-n}{(q-1)q^{2g+1+\frac{n}{2}}} (S(2g+2; n) - qS(2g; n)) = 0.$$

(iii) $n = 2g + 1$: Since $2g + 2 \geq n$, $S(2g + 2; n) = 0$ and we get that

$$\begin{aligned} \langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} &= \frac{n}{(q-1)q^{2g+1+\frac{n}{2}}} \cdot q \cdot S(2g; n) \\ &= \frac{2g+1}{(q-1)q^{3g+\frac{1}{2}}} \cdot S(2g; 2g+1). \end{aligned}$$

Using (2.11),

$$\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} = \frac{2g+1}{(q-1)q^{3g+\frac{1}{2}}} \cdot (\pi_q(2g+1)q^{\frac{(2g+1)-1}{2}}).$$

By replacing $\pi_q(2g+1)$ and simplifying, we obtain

$$\begin{aligned}\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} &= \frac{2g+1}{(q-1)q^{3g+\frac{1}{2}}} \cdot \left(\left(\frac{q^{2g+1}}{2g+1} + O\left(\frac{q^g}{2g+1}\right) \right) q^g \right) \\ &= \frac{q^{\frac{1}{2}}}{q-1} + O(q^{-g}).\end{aligned}$$

(iv) $n = 2g+2$: Similarly,

$$\begin{aligned}\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} &= \frac{n}{(q-1)q^{2g+1+\frac{n}{2}}} \cdot q \cdot S(2g; n) \\ &= \frac{2g+2}{(q-1)q^{3g+1}} \cdot S(2g; 2g+2).\end{aligned}$$

From Theorem 3.1,

$$\begin{aligned}\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} &= \frac{2g+2}{(q-1)q^{3g+1}} \cdot \left(\left(\frac{q^{2g+2}}{2g+2} + O\left(\frac{q^g}{2g+2}\right) \right) (q^g - q^{g-1}) + O(q^{2g}) \right) \\ &= 1 + O(q^{-g}) + O(gq^{-g}).\end{aligned}$$

(v) $n > 2g+2$: We apply Theorem 3.1 to get

$$\begin{aligned}\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} &= \frac{-n}{(q-1)q^{2g+1+\frac{n}{2}}} (S(2g+2; n) - qS(2g; n)) \\ &= \frac{-n}{(q-1)q^{2g+1+\frac{n}{2}}} \left(\pi_q(n)(q^{\frac{2g+2}{2}} - \eta_n q^{2g+2-\frac{n}{2}}) - q \cdot \pi_q(n)(q^{\frac{2g}{2}} - \eta_n q^{2g-\frac{n}{2}}) + O(q^n) \right).\end{aligned}$$

Upon further simplification,

$$\begin{aligned}\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} &= \frac{n}{(q-1)q^{2g+1+\frac{n}{2}}} \left(\eta_n \pi_q(n)(q^{2g+2-\frac{n}{2}} - q^{2g+1-\frac{n}{2}}) + O(q^n) \right) \\ &= \frac{n\eta_n \pi_q(n)}{q^n} + O(nq^{\frac{n}{2}-2g}) \\ &= \eta_n(1 + O(q^{-\frac{n}{2}})) + O(nq^{\frac{n}{2}-2g}).\end{aligned}$$

Note. When $n = 2g+2$, (v) yields (iv).

6. CONTRIBUTION OF THE SQUARES: \square_n

For n even, we have the following contribution from the squares of prime powers:

$$\begin{aligned}
\square_n &= -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P^{2k})=n} \Lambda(P^{2k}) \chi_Q(P^{2k}) \\
&= -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P^k)=\frac{n}{2}} \Lambda(P^k) \chi_Q((P^k)^2) \\
&= -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(h)=\frac{n}{2}} \Lambda(h) \chi_Q(h^2).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\langle \square_n \rangle_{\mathcal{F}_{2g+2}} &= -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P^k)=\frac{n}{2}} \Lambda(P^k) \langle \chi_Q(P^{2k}) \rangle_{\mathcal{F}_{2g+2}} \\
&= -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P^k)=\frac{n}{2}} \deg(P) \frac{1}{(q-1)q^{2g+1}} \sum_{0 \leq \alpha \leq g+1} \sum_{\substack{\deg(A)=\alpha \\ P \nmid A}} \mu(A) \sum_{\substack{\deg(B)=2g+2-2\alpha \\ P \nmid B}} 1.
\end{aligned}$$

Although section 5 shows a slight deviation in $\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}}$ from $\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+1}}$, we will see that $\langle \square_n \rangle_{\mathcal{F}_{2g+2}} = \langle \square_n \rangle_{\mathcal{F}_{2g+1}}$.

Let $m = \deg(P)$. Since

$$\#\{B : \deg(B) = \beta, P \nmid B\} = q^\beta \cdot \begin{cases} 1 & \text{if } m > \beta \\ 1 - \frac{1}{|P|} & \text{if } m \leq \beta, \end{cases}$$

$$\begin{aligned}
\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+1}} &= -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P^k)=\frac{n}{2}} \deg(P) \frac{1}{(q-1)q^{2g+1}} \sum_{0 \leq \alpha \leq g+1} \sum_{\substack{\deg(A)=\alpha \\ P \nmid A}} \mu(A) \sum_{\substack{\deg(B)=2g+2-2\alpha \\ P \nmid B}} 1 \\
&= -\frac{q}{(q-1)q^{\frac{n}{2}}} \sum_{\deg(P^k)=\frac{n}{2}} \deg(P) \cdot \left(\sum_{g+1-\frac{m}{2} < \alpha \leq g+1} \frac{\sigma_m(\alpha)}{q^{2\alpha}} \right. \\
&\quad \left. + \left(1 - \frac{1}{|P|}\right) \cdot \sum_{0 \leq \alpha \leq g+1-\frac{m}{2}} \frac{\sigma_m(\alpha)}{q^{2\alpha}} \right) \\
&= -\frac{q}{(q-1)q^{\frac{n}{2}}} \sum_{\deg(P^k)=\frac{n}{2}} \deg(P) \cdot \left(\left(1 - \frac{1}{|P|}\right) \cdot \sum_{\alpha \geq 0} \frac{\sigma_m(\alpha)}{q^{2\alpha}} \right. \\
&\quad \left. + \sum_{g+1-\frac{m}{2} < \alpha \leq g+1} \frac{\sigma_m(\alpha)}{q^{2\alpha}} - \left(1 - \frac{1}{|P|}\right) \cdot \sum_{\alpha > g+1-\frac{m}{2}} \frac{\sigma_m(\alpha)}{q^{2\alpha}} \right) \\
&= -\frac{q}{(q-1)q^{\frac{n}{2}}} \sum_{\deg(P^k)=\frac{n}{2}} \deg(P) \cdot \left(\left(1 - \frac{1}{|P|}\right) \cdot \sum_{\alpha \geq 0} \frac{\sigma_m(\alpha)}{q^{2\alpha}} \right. \\
&\quad \left. - \sum_{\alpha > g+1} \frac{\sigma_m(\alpha)}{q^{2\alpha}} + \frac{1}{|P|} \cdot \sum_{\alpha > g+1-\frac{m}{2}} \frac{\sigma_m(\alpha)}{q^{2\alpha}} \right) \\
&= -\frac{q}{(q-1)q^{\frac{n}{2}}} \sum_{\deg(P^k)=\frac{n}{2}} \deg(P) \cdot \left(\left(1 - \frac{1}{|P|}\right) \cdot \sum_{\alpha \geq 0} \frac{\sigma_m(\alpha)}{q^{2\alpha}} + O(q^{-2g}) \right).
\end{aligned}$$

Solving the recurrence relation in Lemma 2.1,

$$\begin{aligned}
\langle \square_n \rangle_{\mathcal{F}_{2g+2}} &= -\frac{q}{(q-1)q^{\frac{n}{2}}} \sum_{\deg(P^k)=\frac{n}{2}} \deg(P) \cdot \left(\left(1 - \frac{1}{|P|}\right) \cdot \frac{1 - \frac{1}{q}}{1 - \frac{1}{|P|^2}} + O(q^{-2g}) \right) \\
&= -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P) \mid \frac{n}{2}} \deg(P) \cdot \left(\frac{|P|}{|P|+1} + O(q^{-2g}) \right) \\
&= -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P) \mid \frac{n}{2}} \deg(P) \cdot \left(1 - \frac{1}{|P|+1} + O(q^{-2g}) \right) \\
&= -\frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P) \mid \frac{n}{2}} \deg(P) + \frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P) \mid \frac{n}{2}} \deg(P) \cdot \left(\frac{1}{|P|+1} + O(q^{-2g}) \right).
\end{aligned}$$

Since

$$q^l = \sum_{\deg(h)=l} \Lambda(h) = \sum_{\deg(P^k)=l} \deg(P) = \sum_{\deg(P)|l} \deg(P),$$

$$\langle \square_n \rangle_{\mathcal{F}_{2g+2}} = -1 + \frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P)|\frac{n}{2}} \frac{\deg(P)}{|P|+1} + O(q^{-2g}).$$

7. CONTRIBUTION OF THE HIGHER PRIME POWERS: \mathbb{H}_n

Using trivial bounds for \mathbb{H}_n , we obtain slightly different results from Rudnick in the case where $n > 6g$. This is due to the fact that our estimates of \mathbb{H}_n involve $S(\beta; n)$ for β even, as opposed to β odd, and, from Lemma 2.3,

$$S(\beta; n) \ll \begin{cases} q^{n+\beta} & \text{if } \beta \text{ is even} \\ q^{\frac{n}{2}+\beta} & \text{if } \beta \text{ is odd.} \end{cases}$$

We shall see that our bounds for $n > 6g$ are absorbed in the error term from $\langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}}$ when $n > 2g + 1$.

The contribution to $\text{tr}(\Theta_{C_Q}^n)$ from the higher odd prime powers in (4.1) is:

$$\begin{aligned} \mathbb{H}_n &= -\frac{1}{q^{\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leq d : \text{odd}}} \sum_{\deg(P)=\frac{n}{d}} \frac{n}{d} \chi_Q(P^d) \\ &= -\frac{1}{q^{\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leq d : \text{odd}}} \sum_{\deg(P)=\frac{n}{d}} \frac{n}{d} \chi_Q(P), \end{aligned}$$

where the last equality follows from the fact that $\chi_Q(P^d) = \chi_Q(P)$ for odd d .

This implies that

$$\begin{aligned} \langle \mathbb{H}_n \rangle_{\mathcal{F}_{2g+2}} &= -\frac{1}{(q-1)q^{2g+1+\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leq d : \text{odd}}} \frac{n}{d} \sum_{\deg(P)=\frac{n}{d}} \sum_{2\alpha+\beta=2g+2} \sigma_{\frac{n}{d}}(\alpha) \sum_{\deg(B)=\beta} \left(\frac{B}{P}\right) \\ &= -\frac{1}{(q-1)q^{2g+1+\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leq d : \text{odd}}} \frac{n}{d} \sum_{2\alpha+\beta=2g+2} \sigma_{\frac{n}{d}}(\alpha) S(\beta; \frac{n}{d}). \end{aligned}$$

If $S(\beta; \frac{n}{d}) \neq 0$, then $\beta < \frac{n}{d}$; also, $S(\beta; \frac{n}{d}) \ll q^{\frac{n}{d}+\beta}$. Hence,

$$\begin{aligned}
 \langle \mathbb{H}_n \rangle_{\mathcal{F}_{2g+2}} &\ll \frac{1}{q^{2g+\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leq d : \text{odd}}} \frac{n}{d} \sum_{\beta \leq \min(\frac{n}{d}, 2g+2)} q^{\frac{n}{d}+\beta} \\
 &\ll \frac{n}{q^{2g+\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leq d : \text{odd}}} q^{\frac{n}{d}+\min(2g, \frac{n}{d})}.
 \end{aligned}$$

If $\frac{n}{3} \leq 2g$, then $\min(\frac{n}{d}, 2g) = \frac{n}{d}$ for all $d \geq 3$; and so,

$$\begin{aligned}
 \langle \mathbb{H}_n \rangle_{\mathcal{F}_{2g+2}} &\ll \frac{n}{q^{2g+\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leq d : \text{odd}}} q^{\frac{2n}{d}} \ll \frac{n}{q^{2g+\frac{n}{2}}} \cdot q^{\frac{2n}{3}} = \frac{n}{q^{2g}} \cdot q^{\frac{n}{6}} \\
 &\ll \frac{g}{q^{2g}} \cdot q^g = gq^{-g}.
 \end{aligned}$$

If $\frac{n}{3} > 2g$, then $\min(\frac{n}{d}, 2g) \leq \frac{n}{3}$ for all $d \geq 3$; therefore,

$$\langle \mathbb{H}_n \rangle_{\mathcal{F}_{2g+2}} \ll \frac{n}{q^{2g+\frac{n}{2}}} \cdot q^{\frac{2n}{3}} \ll nq^{\frac{n}{6}-2g}.$$

8. COMPUTING $\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+2}}$

Since $\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+2}} = -\frac{1}{q^{\frac{n}{2}}} + \langle \mathcal{P}_n \rangle_{\mathcal{F}_{2g+2}} + \langle \square_n \rangle_{\mathcal{F}_{2g+2}} + \langle \mathbb{H}_n \rangle_{\mathcal{F}_{2g+2}}$, we obtain the following:

$$\begin{aligned}
 \langle \text{tr} \Theta_{C_Q}^n \rangle_{\mathcal{F}_{2g+2}} &= -\frac{1}{q^{\frac{n}{2}}} + \begin{cases} O(gq^{\frac{-g}{2}}) & 0 < n \leq g+1 \\ 0 & g+1 < n < 2g+1 \\ \frac{q^{\frac{1}{2}}}{q-1} + O(q^{-g}) & n = 2g+1 \\ \eta_n(1 + O(q^{\frac{-n}{2}})) + O(nq^{\frac{n}{2}-2g}) & 2g+1 < n \end{cases} \\
 &\quad + \eta_n(-1 + \frac{1}{q^{\frac{n}{2}}} \sum_{\deg(P) \mid \frac{n}{2}} \frac{\deg(P)}{|P|+1} + O(q^{-2g})) \\
 &\quad + \begin{cases} O(gq^{-g}) & n \leq 6g \\ O(nq^{\frac{n}{6}-2g}) & 6g < n. \end{cases}
 \end{aligned}$$

In particular,

Theorem 8.1.

$$\begin{aligned} \langle \text{tr } \Theta_{C_Q}^n \rangle_{\mathcal{F}_{2g+2}} &= -\frac{1}{q^{\frac{n}{2}}} + \eta_n \frac{1}{q^{\frac{n}{2}}} \cdot \sum_{\deg(P) \mid \frac{n}{2}} \frac{\deg(P)}{|P|+1} + O(gq^{\frac{-g}{2}}) \\ &\quad + \begin{cases} -\eta_n & 0 < n < 2g+1 \\ \frac{q^{\frac{1}{2}}}{q-1} & n = 2g+1 \\ O(nq^{\frac{n}{2}-2g}) & 2g+1 < n. \end{cases} \end{aligned}$$

9. COMPUTING $\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2}}$

From [1], we have the following:

Theorem 9.1.

$$\langle \text{tr } \Theta_{C_Q}^n \rangle_{\mathcal{F}_{2g+1}} = \eta_n \frac{1}{q^{\frac{n}{2}}} \cdot \sum_{\deg(P) \mid \frac{n}{2}} \frac{\deg(P)}{|P|+1} + O(gq^{-g}) + \begin{cases} -\eta_n & 0 < n < 2g \\ -1 - \frac{1}{q-1} & n = 2g \\ O(nq^{\frac{n}{2}-2g}) & 2g < n. \end{cases}$$

We would like to find the expected value of $\text{tr}(\Theta_{C_Q}^n)$ over all curves $C_Q : y^2 = Q(x)$ of genus g with Q monic. To do this, we use Theorems 8.1 and 9.1. By identifying the family of curves described above with $\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2}$, we see that

$$\begin{aligned} &\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2}} \\ &= \frac{\#\mathcal{F}_{2g+1}}{\#(\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2})} \langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+1}} + \frac{\#\mathcal{F}_{2g+2}}{\#(\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2})} \langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+2}}, \end{aligned}$$

where

$$\begin{aligned} \#(\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2}) &= \#\mathcal{F}_{2g+1} + \#\mathcal{F}_{2g+2} \\ &= (q-1)q^{2g} + (q-1)q^{2g+1} \\ &= q^{2g}(q-1)(q+1). \end{aligned}$$

We obtain the following:

Corollary 9.2.

$$\begin{aligned} \langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2}} &= -\frac{1}{q^{\frac{n}{2}}} \frac{q}{q+1} + \eta_n \frac{1}{q^{\frac{n}{2}}} \cdot \sum_{\deg(P) \mid \frac{n}{2}} \frac{\deg(P)}{|P|+1} + O(gq^{\frac{-g}{2}}) \\ &\quad + \begin{cases} -\eta_n & 0 < n < 2g \\ -1 - \frac{1}{q^2-1} & n = 2g \\ \frac{q^{\frac{3}{2}}}{q^2-1} & n = 2g+1 \\ O(nq^{\frac{n}{2}-2g}) & 2g+1 < n. \end{cases} \end{aligned}$$

Note. The first main term in Corollary 9.2 does not appear in Theorem 9.1, neither does the term $\frac{q^{\frac{3}{2}}}{q^2-1}$ corresponding to $n = 2g + 1$. Similarly, for $n = 2g$, the constant $\frac{1}{q-1}$ in Theorem 9.1 is scaled down to $\frac{1}{q^2-1}$ in Corollary 9.2. In the next section, we shall see that these differences are diminished when we consider the average of $\text{tr}(\Theta_{C_Q}^n)$ over \mathcal{H}_g .

10. COMPUTING $\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g}$

As we mentioned in the introduction, averaging over monic squarefree polynomials of a fixed degree is not the same as averaging over the moduli space of hyperelliptic curves of genus g : in the latter case, we consider polynomials of degree $2g + 1$ and $2g + 2$. Also, by restricting ourselves to monic polynomials, we introduce a bias in the average value of the trace: the contribution of the point at infinity is related to the leading coefficient of Q , as seen by equation (2.4).

We now turn our attention to finding the average of $\text{tr}(\Theta_{C_Q}^n)$ over \mathcal{H}_g : from equations (1.5) and (2.4),

$$(10.1) \quad \langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} = \frac{1}{\#\mathcal{H}_g} \cdot \sum_{Q \in \mathcal{H}_g} \left(-\frac{\lambda_Q^n}{q^{\frac{n}{2}}} - \frac{1}{q^{\frac{n}{2}}} \sum_{\deg(f)=n} \Lambda(f) \chi_Q(f) \right),$$

where

$$\lambda_Q = \begin{cases} -1 & \text{if } \deg(Q) \text{ is even and } \text{sgn}(Q) \neq \square \\ 0 & \text{if } \deg(Q) \text{ is odd} \\ 1 & \text{if } \deg(Q) \text{ is even and } \text{sgn}(Q) = \square. \end{cases}$$

Since there are exactly $(q-1)/2$ squares and $(q-1)/2$ non-squares in \mathbb{F}_q^* , if n is odd,

$$\frac{1}{\#\mathcal{H}_g} \cdot \sum_{Q \in \mathcal{H}_g} \lambda_Q^n = \frac{1}{\#\mathcal{H}_g} \cdot \sum_{Q \in \mathcal{H}_g} \lambda_Q = 0.$$

On the other hand, if n is even,

$$\frac{1}{\#\mathcal{H}_g} \cdot \sum_{Q \in \mathcal{H}_g} \lambda_Q^n = \frac{1}{\#\mathcal{H}_g} \cdot \sum_{Q \in \mathcal{H}_g} |\lambda_Q| = \frac{\#\widehat{\mathcal{F}}_{2g+2}}{\#\mathcal{H}_g} = \frac{q}{q+1}.$$

Also, given $D \in \mathbb{F}_q[x]$ with $\deg(D) = d$, we may write $D = A^2B$, where $A, B \in \mathbb{F}_q[x]$ with A monic, B not necessarily monic, and $\deg(A) = \alpha$, $\deg(B) = \beta$, so that $d = 2\alpha + \beta$. From here, we can take the character sum above over

all elements in $\mathbb{F}_q[x]$ of genus g by sieving out the squarefree terms (as we did earlier):

$$\begin{aligned}
\sum_{Q \in \mathcal{H}_g} \chi_Q(f) &= \sum_{\substack{2\alpha+\beta=d \\ d=2g+1, 2g+2}} \sum_{\substack{\deg(B)=\beta \\ B \text{ n.n.m.}}} \sum_{\deg(A)=\alpha} \mu(A) \left(\frac{A}{f}\right)^2 \left(\frac{B}{f}\right) \\
&= \sum_{\substack{2\alpha+\beta=d \\ d=2g+1, 2g+2}} \sigma(f; \alpha) \sum_{\substack{\deg(B)=\beta \\ B \text{ n.n.m.}}} \left(\frac{B}{f}\right) \\
&= \sum_{\substack{2\alpha+\beta=d \\ d=2g+1, 2g+2}} \sigma(f; \alpha) \sum_{a \in \mathbb{F}_q^*} \sum_{\deg(B)=\beta} \left(\frac{aB}{f}\right) \\
&= \sum_{\substack{2\alpha+\beta=d \\ d=2g+1, 2g+2}} \sigma(f; \alpha) \sum_{a \in \mathbb{F}_q^*} \sum_{\deg(B)=\beta} \left(\frac{a}{f}\right) \cdot \left(\frac{B}{f}\right) \\
&= \sum_{a \in \mathbb{F}_q^*} \left(\frac{a}{f}\right) \sum_{\substack{2\alpha+\beta=d \\ d=2g+1, 2g+2}} \sigma(f; \alpha) \sum_{\deg(B)=\beta} \left(\frac{B}{f}\right).
\end{aligned}$$

Hence,

$$\begin{aligned}
\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} &= \\
&- \frac{1}{q^{\frac{n}{2}} \cdot \#\mathcal{H}_g} \left(\sum_{Q \in \mathcal{H}_g} \lambda_Q^n + \sum_{\deg(f)=n} \Lambda(f) \sum_{a \in \mathbb{F}_q^*} \left(\frac{a}{f}\right) \sum_{\substack{2\alpha+\beta=d \\ d=2g+1, 2g+2}} \sigma(f; \alpha) \sum_{\deg(B)=\beta} \left(\frac{B}{f}\right) \right).
\end{aligned}$$

If f is a power of some prime in $\mathbb{F}_q[x]$, say $f = P^k$, then for all $a \in \mathbb{F}_q^*$ (see Proposition 3.2 of [2]),

$$\left(\frac{a}{f}\right) = \left(\frac{a}{P}\right)^k = \left(a^{\frac{q-1}{2} \deg(P)}\right)^k = a^{\frac{q-1}{2} \deg(f)}.$$

If $\deg(f) = \deg(P^k) = n$ is even, then $\left(\frac{a}{f}\right) = 1$ because $|\mathbb{F}_q^*| = q - 1$. This tells us that $\sum_{a \in \mathbb{F}_q^*} \left(\frac{a}{f}\right) = q - 1$. If $\deg(f) = \deg(P^k) = n$ is odd, then we have that $\sum_{a \in \mathbb{F}_q^*} \left(\frac{a}{f}\right) = 0$ because there are exactly $(q - 1)/2$ QR in \mathbb{F}_q^* and exactly $(q - 1)/2$ NQR in \mathbb{F}_q^* .

So, for n odd,

$$\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} = 0,$$

and for n even,

$$\begin{aligned}
& \langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} \\
&= -\frac{1}{q^{\frac{n}{2}}} \frac{q}{q+1} - \frac{1}{\#\mathcal{H}_g \cdot q^{\frac{n}{2}}} \sum_{\deg(f)=n} \Lambda(f) \sum_{a \in \mathbb{F}_q^*} \left(\frac{a}{f}\right) \sum_{\substack{2\alpha+\beta=d \\ d=2g+1, 2g+2}} \sigma(f; \alpha) \sum_{\deg(B)=\beta} \left(\frac{B}{f}\right) \\
&= -\frac{1}{q^{\frac{n}{2}}} \frac{q}{q+1} - \frac{1}{\#(\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2}) \cdot q^{\frac{n}{2}}} \sum_{\deg(f)=n} \Lambda(f) \sum_{\substack{2\alpha+\beta=d \\ d=2g+1, 2g+2}} \sigma(f; \alpha) \sum_{\deg(B)=\beta} \left(\frac{B}{f}\right) \\
&= -\frac{1}{q^{\frac{n}{2}}} \frac{q}{q+1} - \frac{1}{q^{\frac{n}{2}}} \sum_{\deg(f)=n} \Lambda(f) \langle \chi_Q(f) \rangle_{\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2}}.
\end{aligned}$$

In other words,

Theorem 10.1. *For n odd,*

$$\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} = 0,$$

and for n even,

$$\begin{aligned}
& \langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} = \langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{F}_{2g+1} \cup \mathcal{F}_{2g+2}} \\
&= \frac{1}{q^{\frac{n}{2}}} \cdot \sum_{\substack{\deg(P) \mid \frac{n}{2} \\ \deg(P) \neq 1}} \frac{\deg(P)}{|P|+1} + O(gq^{-\frac{g}{2}}) + \begin{cases} -1 & 0 < n < 2g \\ -1 - \frac{1}{q^2-1} & n = 2g \\ O(nq^{\frac{n}{2}-2g}) & 2g < n. \end{cases}
\end{aligned}$$

In particular,

Corollary 10.2. *If n is odd, then*

$$\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} = \int_{\text{USp}(2g)} \text{tr}(U^n) dU.$$

For n even with $3 \log_q(g) < n < 4g - 5 \log_q(g)$ and $n \neq 2g$,

$$\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} = \int_{\text{USp}(2g)} \text{tr}(U^n) dU + o\left(\frac{1}{g}\right).$$

Proof. The first part is clear. To prove the second part, we treat each non-main term in Theorem 10.1 separately and show that each of them contributes an error term of $o(\frac{1}{g})$ in the desired region.

Fix $\epsilon > 0$. If $n < 4g - (4 + \epsilon) \log_q(g)$, then

$$\lim_{g \rightarrow \infty} g \cdot nq^{\frac{n}{2}-2g} \leq \lim_{g \rightarrow \infty} g^2 g^{-2-\frac{\epsilon}{2}} = \lim_{g \rightarrow \infty} g^{-\frac{\epsilon}{2}} = 0;$$

i.e.,

$$O(nq^{\frac{n}{2}-2g}) = o(\frac{1}{g}).$$

Note that

$$\frac{1}{q^{\frac{n}{2}}} \sum_{\substack{\deg(P) \mid \frac{n}{2} \\ \deg(P) \neq 1}} \frac{\deg(P)}{|P| + 1} = O(\frac{n}{q^{\frac{n}{2}}}).$$

If $n = (2 + \epsilon) \log_q(g)$, then

$$\lim_{g \rightarrow \infty} g^{\frac{n}{q^{\frac{n}{2}}}} \ll_{\epsilon} \lim_{g \rightarrow \infty} \frac{g \log_q(g)}{g^{1+\frac{\epsilon}{2}}} = 0.$$

So, for $n > (2 + \epsilon) \log_q(g)$,

$$\frac{1}{q^{\frac{n}{2}}} \sum_{\substack{\deg(P) \mid \frac{n}{2} \\ \deg(P) \neq 1}} \frac{\deg(P)}{|P| + 1} = O(\frac{n}{q^{\frac{n}{2}}}) = o(\frac{1}{g}).$$

We have actually shown a stronger version of our statement; namely, for any fixed $\epsilon > 0$ and for any even n with $(2 + \epsilon) \log_q(g) < n < 4g - (4 + \epsilon) \log_q(g)$ and $n \neq 2g$,

$$\langle \text{tr}(\Theta_{C_Q}^n) \rangle_{\mathcal{H}_g} = -1 + o(\frac{1}{g}).$$

□

We now look at another approach which quickly verifies the first result of Theorem 10.1. This argument was provided by Dr. Zeév Rudnick: fix a finite field \mathbb{F}_q of odd cardinality q , let Q be any monic, squarefree polynomial in $\mathbb{F}_q[x]$ of degree $2g + 1$ or $2g + 2$, and let $a \in \mathbb{F}_q^*$. Then

$$\begin{aligned} \#C(\mathbb{F}_{q^n}) &= \sum_{x_0 \in \mathbb{P}^1(\mathbb{F}_{q^n})} \left(\chi_n(a(Q(x_0))) + 1 \right) \\ &= q^n + 1 + \sum_{x_0 \in \mathbb{P}^1(\mathbb{F}_{q^n})} \chi_n(a(Q(x_0))), \end{aligned}$$

where χ_n is a multiplicative character on \mathbb{F}_{q^n} defined by

$$\chi_n(\alpha) := \begin{cases} 1 & \text{if } \alpha \text{ is a square in } \mathbb{F}_{q^n}^* \\ 0 & \text{if } \alpha = 0 \\ -1 & \text{if } \alpha \text{ is not a square in } \mathbb{F}_{q^n}^*. \end{cases}$$

When x_0 is the point at infinity, $Q(x_0)$ is defined by the evaluation of $x^{2g+2}Q(\frac{1}{x})$ at $x = 0$; i.e., $\chi_n(Q(\infty))$ yields λ_Q according to the count of (1.4). Moreover,

$$-q^{\frac{n}{2}} \operatorname{tr}(\Theta_C^n) = \sum_{x_0 \in \mathbb{P}^1(\mathbb{F}_{q^n})} \chi_n(aQ(x_0))$$

Therefore,

$$\begin{aligned} \langle \operatorname{tr}(\Theta_C^n) \rangle_{\mathcal{H}_g} &= \frac{-1}{q^{\frac{n}{2}} \# \mathcal{H}_g} \sum_{a \in \mathbb{F}_q^*} \sum_{Q \in \mathbb{F}_q[x]} ' \sum_{x_0 \in \mathbb{P}^1(\mathbb{F}_{q^n})} \chi_n(aQ(x_0)) \\ &= \frac{-1}{q^{\frac{n}{2}} \# \mathcal{H}_g} \sum_{a \in \mathbb{F}_q^*} \chi_n(a) \sum_{Q \in \mathbb{F}_q[x]} ' \sum_{x_0 \in \mathbb{P}^1(\mathbb{F}_{q^n})} \chi_n(Q(x_0)), \end{aligned}$$

where $\sum_{Q \in \mathbb{F}_q[x]} '$ indicates that the sum is over all monic, squarefree polynomials $Q \in \mathbb{F}_q[x]$ such that $\deg(Q) = 2g + 1$ or $\deg(Q) = 2g + 2$. When n is odd, there are exactly $\frac{q-1}{2}$ squares and $\frac{q-1}{2}$ non-squares in $\mathbb{F}_q^* \subset \mathbb{F}_{q^n}$, which tells us that

$$\sum_{a \in \mathbb{F}_q^*} \chi_n(a) = 0.$$

So, for odd n ,

$$\langle \operatorname{tr}(\Theta_C^n) \rangle_{\mathcal{H}_g} = 0.$$

On the other hand, when n is even, computing the average over the entire moduli space reduces to computing the average over the moduli space with the restriction that $a = 1$: for even n , every element of \mathbb{F}_q^* is a square in $\mathbb{F}_{q^n}^*$ so that

$$\sum_{a \in \mathbb{F}_q} \chi_n(a) = q - 1$$

and

$$\begin{aligned} \langle \operatorname{tr}(\Theta_C^n) \rangle_{\mathcal{H}_g} &= -\frac{(q-1)}{q^{\frac{n}{2}} \# \mathcal{H}_g} \sum_{Q \in \mathbb{F}_q[x]} ' \sum_{x_0 \in \mathbb{P}^1(\mathbb{F}_{q^n})} \chi_n(Q(x_0)) \\ &= \langle \operatorname{tr}(\Theta_C^n) \rangle_{\widehat{\mathcal{H}}_g}, \end{aligned}$$

where

$$\widehat{\mathcal{H}}_g := \{C_Q \in \mathcal{H}_g : Q \text{ monic}\}.$$

Evidently, $\# \mathcal{H}_g = (q-1) \# \widehat{\mathcal{H}}_g$.

11. ACKNOWLEDGEMENTS

We thank Dr. Chantal David for many valuable suggestions which have vastly improved this paper and for her continuous support throughout this research. We also thank Dr. Zeév Rudnick and Manal Alzahrani for their valuable input and insight.

REFERENCES

- [1] Rudnick, Z., *Traces of High Powers of the Frobenius Class in the Hyperelliptic Ensemble*, Acta Arith., 143(1):81-99, 2010.
- [2] Rosen, M., *Number Theory in Function Fields*, Springer-Verlag, New York, 2002.
- [3] Diaconis, P. and Shahshahani, M., *On the Eigenvalues of Random Matrices*, Studies in Applied Probabilities, J. Appl. Probab. 31A: 49-62, 1994.
- [4] Bucur, A., David, C., Feigon, B., Kaplan, N., Lalin, M., Ozman, E., and Matchett Wood, M., *The Distribution of \mathbb{F}_q -Points on Cyclic l -Covers of Genus g* , 2014.
- [5] Alzahrani, M., *The Distribution of Points on Hyperelliptic Curves Over \mathbb{F}_q of Genus g in Finite Extensions of \mathbb{F}_q* (Master's Thesis), Concordia University, Canada, 2015.
- [6] Kurlberg, P. and Rudnick, Z., *The Fluctuations in the Number of Points on a Hyperelliptic curve over a Finite Field*, Journal of Number Theory 129, no. 3 (2009):580-87.
- [7] Weil, A., *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publications de l'Institut de Mathématique de l'Université de Strasbourg 7, Paris: Hermann et Cie., 1948.
- [8] Silverman, J., *The Arithmetic of Elliptic Curves*, Springer, Dordrecht, 2009.
- [9] Meleleo, G., *Questions Related to Primitive Points on Elliptic Curves and Statistics for Biquadratic Curves Over Finite Fields* (Ph. D. Thesis), Università degli Studi Roma Tre, Italy, 2015. Retrieved from http://www.matfis.uniroma3.it/dottorato/TESI/meleleo/2015_04_30-Tesi_Meleleo.pdf.